DISA Public Key Infrastructure Strategy

AFCEA Tech Net Cyber 2019

Donald R. Parker Jr.
DISA ID21 PKI Branch Chief
May 16, 2019

PKI Program Management Office

MISSION

DOD PKI provides for the generation, production, distribution, control, revocation, recovery, and tracking of public key certificates and their corresponding private keys. DOD PKI supports the secure flow of information across the DOD Information Networks as well as secure local storage of information.
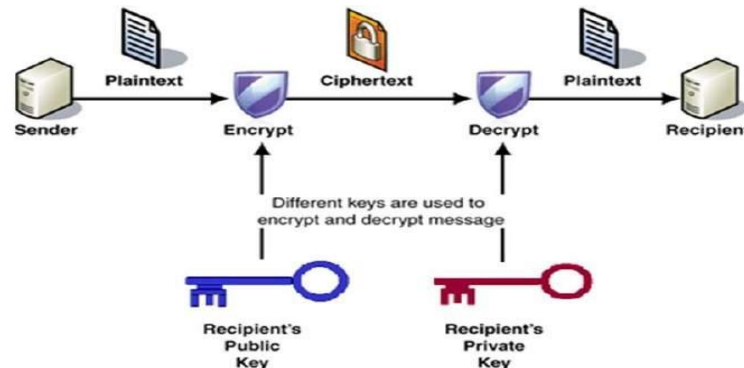
Way Ahead for "Evolving PKI"
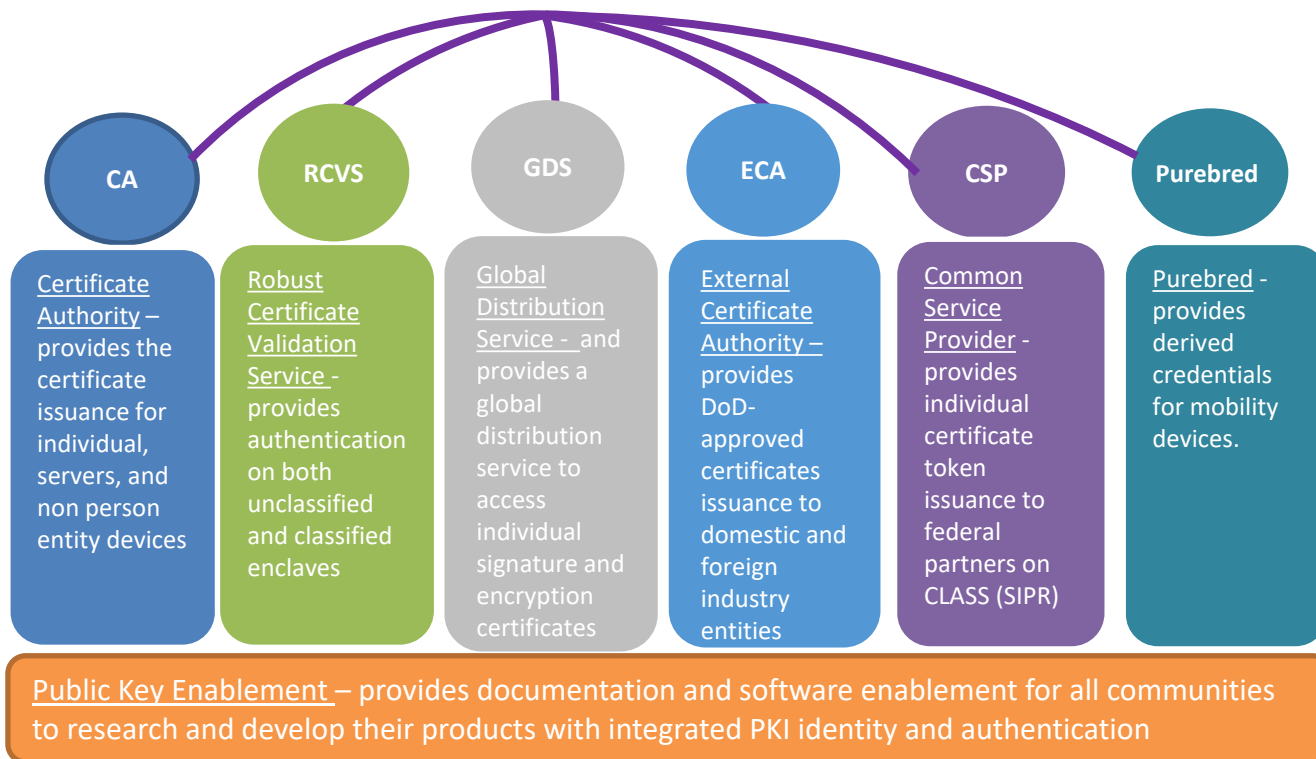Non Person-Entity
Mobile Credentialing

Why PKI Matters

- PKI has emerged as the foundation that is being utilized to provide secure transmission of data and Internet security by providing the cornerstones of security:

    - Identification and Authentication
    - Data Integrity
    - Confidentiality
    - Technical Non-Repudiation

- The elements combine to provide a secure, non-breakable environment for any type of electronic transactions.
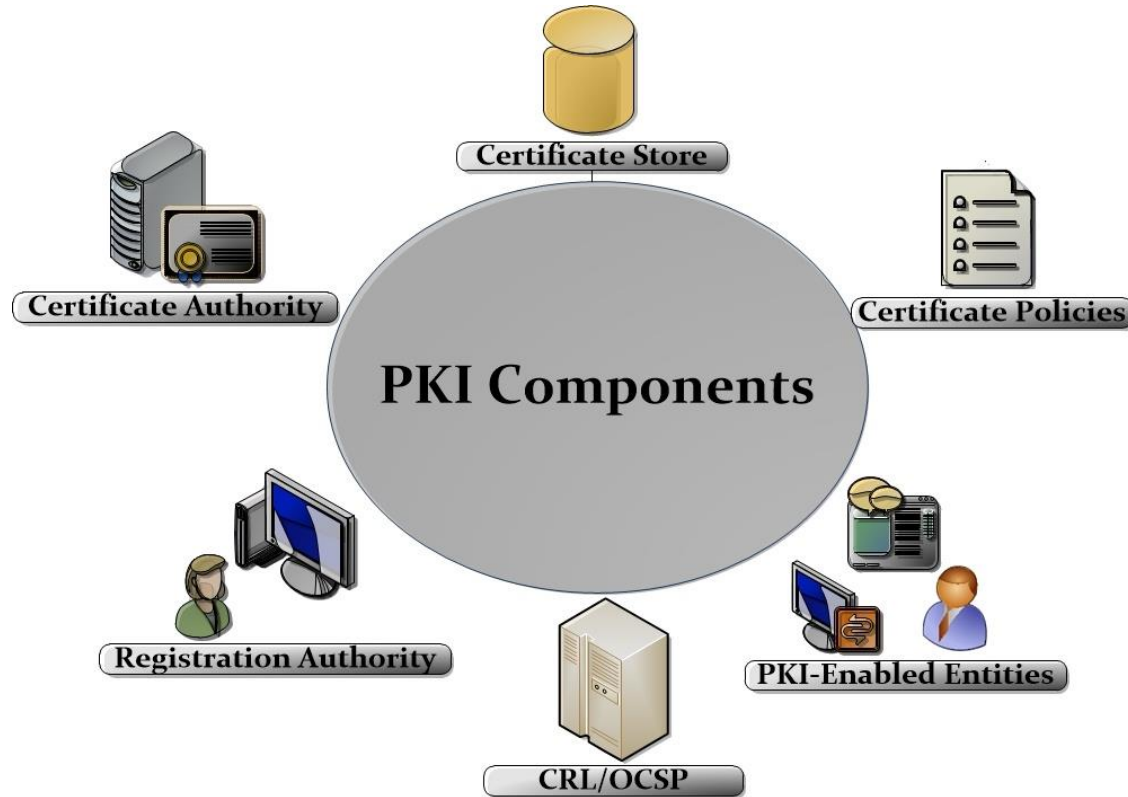
DoD PKI Capabilities

DoD Certificate Infrastructure for the Department of Defense

CA	RCVS	GDS	ECA	CSP	Purebred
Certificate Authority – provides the certificate issuance for individual, servers, and non person entity devices	Robust Certificate Validation Service - provides authentication on both unclassified and classified enclaves	Global Distribution Service - and provides a global distribution service to access individual signature and encryption certificates	External Certificate Authority – provides DoD-approved certificates issuance to domestic and foreign industry entities	Common Service Provider - provides individual certificate token issuance to federal partners on CLASS (SIPR)	Purebred - provides derived credentials for mobility devices.

Public Key Enablement – provides documentation and software enablement for all communities to research and develop their products with integrated PKI identity and authentication
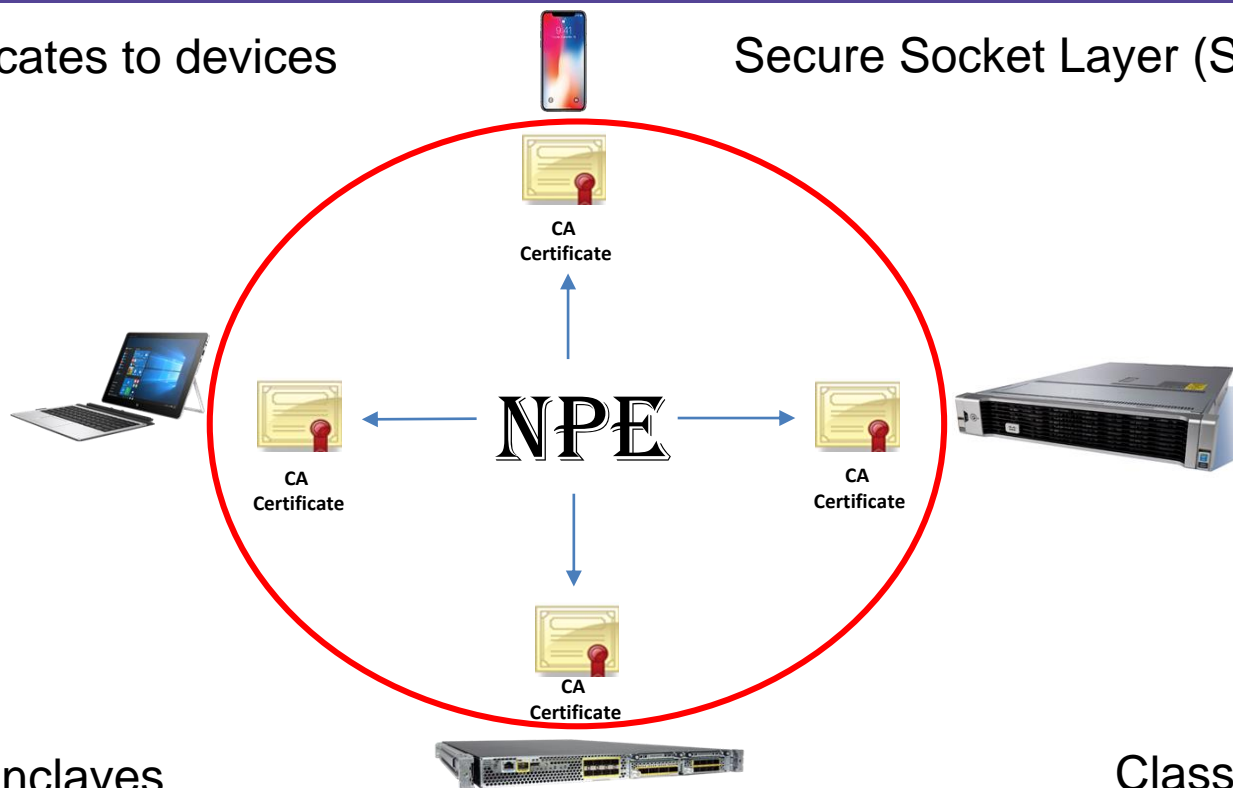
PKI System Elements

DOD PKI Non Person-Entity (NPE)

Provides certificates to devices

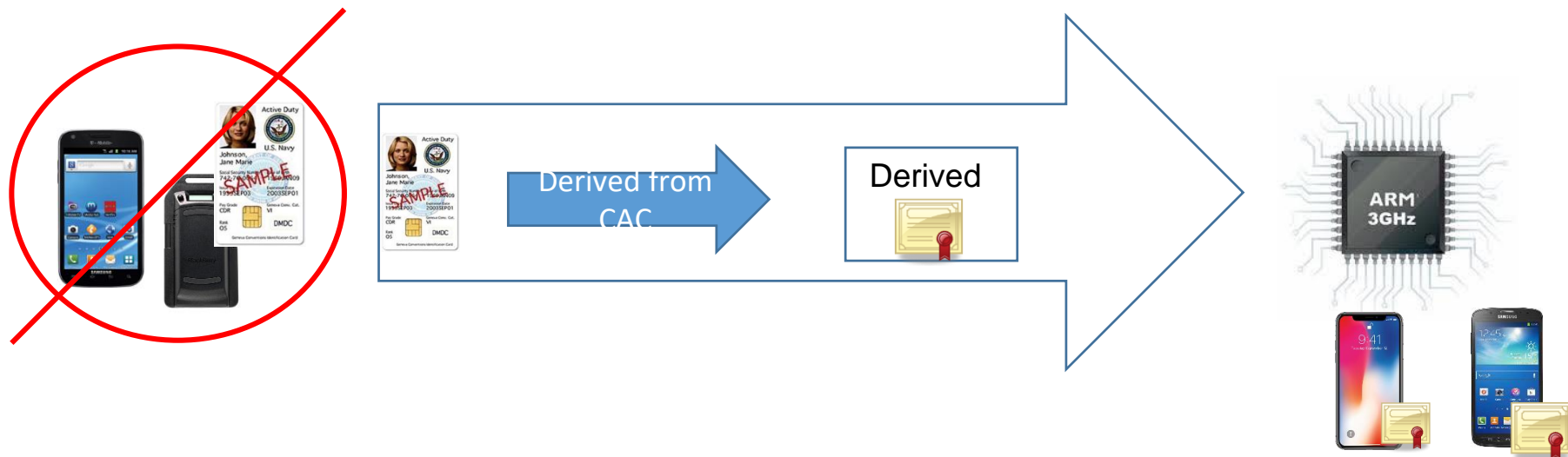Secure Socket Layer (SSL) certificates

Unclassified Enclaves

Classified enclaves

Mobile Credentialing Update

Purebred and Mobile Derived Credentials

Purebred issued derived credentials enable CAC holders an alternative form factor to utilize signed and encrypted email and secure web browsing to CAC enabled websites without a reader or sled
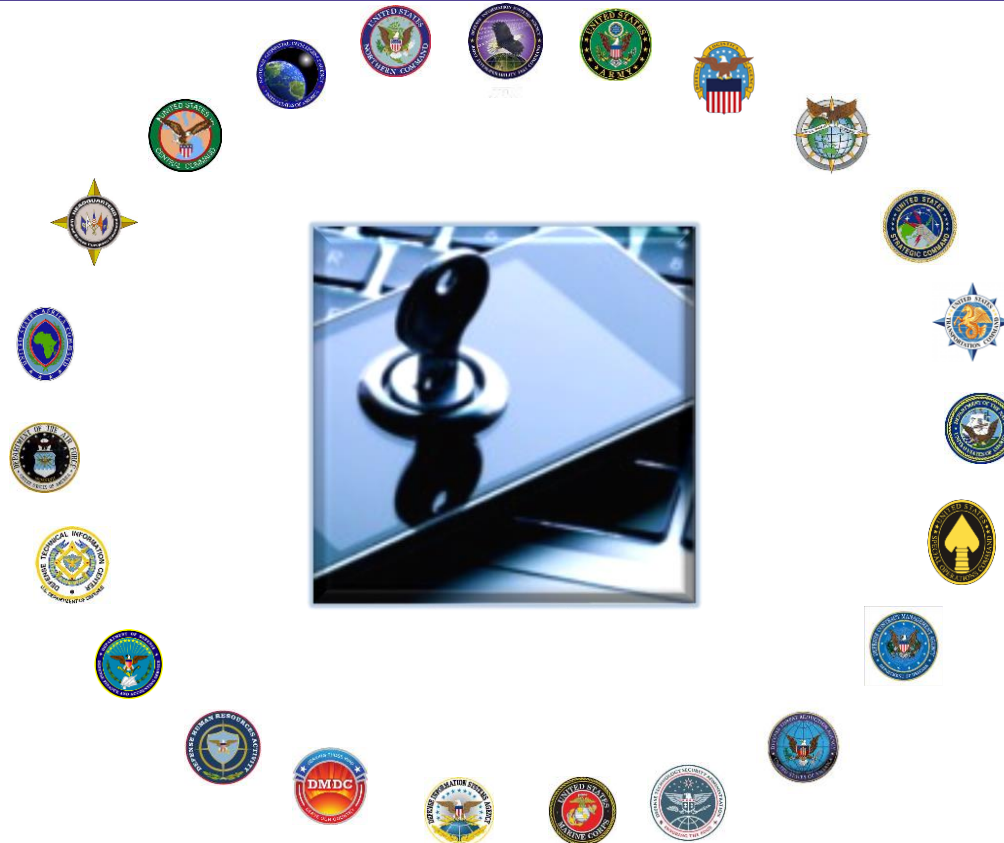
Supported Devices

- Apple iOS Devices (all latest iPhone & iPad models)
  98,537 Devices

- Android (Android 6/Marshmallow and above)
  11,133 Devices
  - Samsung Knox
  - Android for Work

- Windows 10 Tablets with validated TPM 2.0 chipsets
  57 Devices

- Yubikey 4+ Security Tokens
  47 Devices

Purebred Customers & Metrics

Devices: 109,835

Agents: 4,284

Purebred Credentials for Mobile Devices

- Contact your service desk or mobility management service provider to determine if Purebred is offered

- If a DoD Mobility Unclassified Capability (DMUC) customer, contact to your Tier I service desk
  - You may need to be migrated to Email+ on iOS (a new mobile email client)
  - https://disa.deps.mil/ext/cop/dod_mobility/DC_Purebred/SitePages/Home.aspx

- If you manage mobile device for your organization and do not offer Purebred to your users, contact the PKI team to onboard your organization
  - dodpke@mail.mil
  - https://iase.disa.mil/pki-pke/Pages/purebred.aspx

Your mobile device management capability service provider provides the Purebred app and registration services (agent duties)

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

💻 **www.disa.mil**   f **/USDISA**   🐦 **@USDISA**

visit us

DISA
Booth 1929

follow us

f Facebook/USDISA

Twitter/USDISA

meet with us

Industry partners can request a meeting with DISA by completing a form at **www.disa.mil/about/industry-partners**.